REMARKS

A review of the claims indicates that:

A) Claims 1—82 are cancelled.

B) Claims 83—124 are new.

In view of the following remarks, Applicant respectfully requests allowance of the new claims.

Discussion of §103 Issues

Claims 83—124 are new. Full support for these claims is found in Figs. 3 and 4, in the discussion of these figures, and in other locations. In order to move the prosecution of this application forward, the Applicant addresses §103 issues associated with U.S. Patent No. 6,079,018 (hereinafter "Hardy") and U.S. Patent No. 6,453,416 (hereinafter "Epstein").

The §103 Standard

To establish a *prima facie* case of obviousness, three basic criteria *must* be met. MPEP § 2142. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992); *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Second, there must be a reasonable expectation of success. *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

Hence, when patentability turns on the question of obviousness, the search for, and analysis of, the prior art includes evidence relevant to the finding of

whether there is a teaching, motivation, or suggestion to select and combine or modify the references relied on as evidence of obviousness. The need for specificity pervades this authority. See, e.g., *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000) ("particular findings must be made as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed").

Discussion of §103 Issues

The Applicant herein addresses issues related to the Section 103 rejection of Claim 3 that may be relevant to the new claims.

Claim 83 recites a method, at least partially implemented by a computer, comprising:

- **building a data block comprising a first random value and a cryptographic hash of the first random value;**
- generating, on a second computing device, a signature by digitally signing a string containing a second random value; and
- computing an encryption key, for encrypting the data block, by hashing a combination of the signature and a third random value.

The Hardy reference discloses five (5) embodiments for generating unique secure values for digitally signing documents. In none of these embodiments does Hardy teach or suggest *building a data block* comprising a first random value and a cryptographic hash *of the first random value*. In particular, Hardy teaches the Prior Art method for signing documents, at FIG. 1. Additionally, Hardy teaches four embodiments—seen at FIGS. 3 through 6—that teach Hardy's advancements in this area.

Hardy's advancements include a method of deriving a pseudo random key, known as "k". The pseudo random key k is mentioned at column 8, lines 22—23,

and is seen as the "middle variable" input to the signature generation procedure 148. (Note that this procedure is mentioned without the typo seen in the FIGS. 3—6 of the drawings at column 10, lines 45—46 and other locations.) In operation, k is used along with a private key "x" and a hash "H" of the document in a known "signature generating procedure" (e.g. DSA) to create a "digital signature".

Hardy does not teach or suggest, "building a data block comprising a first random value and a cryptographic hash of the first random value". The Applicant will now review the locations wherein Hardy teaches the use of random values, and the locations wherein Hardy teaches hashed values. By way of this review, it will be seen that Hardy does not teach or suggest the combination of a random value and the hash *of the random value* in a data block.

Referring to the Hardy reference, Hardy uses random values in several locations. In FIG. 1, Hardy teaches that the key "k" can be random (see Hardy, column 1, lines 60—65). In operation, Hardy pairs the key "k" with the private key "x" and the hash of the document (not the hash of the key "k"). Thus, Hardy uses these values as input to the digital signature algorithm, and does not teach or suggest *creation of a data block comprising a random value and a hash of the random value.*

Referring to FIG. 3 of Hardy, creates the key k1, which appears to be the same as the pseudo random key k of FIG. 1. However, Hardy pairs the key "k1" with the hash H of the document 52. Thus, Hardy does not teach or suggest

forming a data block with a random value and its hash. Instead, Hardy creates "k1" and pairs it with the hash *of the document*. Thus, Hardy does not teach the random value and the hash of the random value. Moreover, Hardy does not disclose creation of a data block; instead, Hardy teaches using the values as input to the hash procedure 146.

Continuing to refer to FIG. 3, Hardy additionally teaches the creation of the pseudo random key "k". However, Hardy teaches (same as FIG. 1) that the key "k" is combined with the hash of the document "H" and the private key "x". These three data are used as input to the signature generating procedure 148. Thus, Hardy does not teach, "building a data block comprising a first random value and a cryptographic hash of the first random value".

Referring to FIGS. 4—6 of Hardy, it can be seen that Hardy continues to teach that a random or pseudo random value (e.g. "k") can be combined with a hashed value. However, Hardy fails to teach a data block having a random value and a hash of that random value. For example, while Hardy teaches that "k" can be a random value, Hardy fails to teach or suggest that "k" can be combined with the hash of "k" to form a data block. Instead, "k" is used with the hash "H" of the document 52.

In the rejection of Claim 3, the Patent Office suggested that the random value "k" and the hash "H" (by hash procedure 146) of the document 52 taught and/or suggested the elements of the Applicant's claim. The Applicant respectfully disagrees.

In fact, Claim 83 recites, a data block comprising "a first random value and a cryptographic hash of the first random value". That is, the data block includes a random value and a cryptographic hash of *that* random value.

In contrast, as the Patent Office points out, Hardy teaches that the random value "k" is combined with the hash "H" of the document—and not with the hash of "k". In fact, Hardy does not teach that "k" is hashed, let alone that the hash of "k" is combined with "k".

Therefore, Hardy does not teach or suggest, "building a data block that includes a first random value and a cryptographic hash of the first random value". Accordingly, the Applicant respectfully requests that the Patent Office withdraw the argument against original Claim 3, and allow new Claim 83 and its dependent claims.

Claims 84—91 depend from Claim 83 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features that, in combination with those recited in Claim 84, are neither disclosed nor suggested in references of record, either singly or in combination with one another.

Claim 92 recites a method, at least partially implemented by a computer, comprising:

- accessing an encrypted data block, **wherein the encrypted data block comprises an encryption of a combination of a first random value and a hash of the first random value**;
- accessing second and third random values;
- providing a string containing the second random value to a second computing device;
- generating, on the second computing device, a signature by digitally signing the string containing the second random value; and
- computing a decryption key, configured to decrypt the encrypted data block, wherein computing the decryption key uses the signature generated on the second computing device and the third random value.

As seen in the discussion of Hardy, above with respect to Claim 83, Hardy does not teach or suggest a data block comprising "an encryption of a first random value and a hash of the first random value". Instead, Hardy teaches random values, such as the pseudo random key "k". Additionally, Hardy teaches use of a hash function. For example, (referring to FIG. 3) Hardy teaches that the document 52 is hashed and that the intermediate value "k2" is hashed to result in the pseudo random key "k".

However, Hardy does not teach accessing an encrypted data block, wherein the encrypted data block comprises an encryption of a random value *and a hash of that random value.*

As seen above in the discussion of Claim 83, in addressing rejection of Claim 3, the Patent Office suggests that the association of the random key "k" and the hash "H" of the document 52 meets the elements recited in the claims. However, the Applicant must respectfully disagree.

In fact, the document 52 is different from the key "k". Therefore, the hash of "k" will be different from the hash "H" of the document 52. Accordingly, the combination of the key "k" and the hash of the document 52 is not the same as would be the case if Hardy had taught or suggested combining the key "k" with the hash of the key "k". However, such a step would not fit into the algorithm taught by Hardy, nor would Hardy's algorithm suggest such as step. In fact, there is no use for the hash of the key "k" in Hardy's algorithm, and Hardy does not teach or suggest that "k" be hashed, let alone hashed and combined with "k" in a data block.

Accordingly, Hardy does not teach or suggest a data block comprising an encryption of a first random value and a hash of that value.

In the prior Office Action, the Patent Office addressed this issue with respect to Claim 3. The Applicant respectfully disagrees with the Patent Office's conclusions. Accordingly, the Applicant incorporates herein, by reference, the discussion seen with respect to Claim 83, above.

Therefore, Hardy does not teach or suggest, "accessing an encrypted data block, wherein the encrypted data block comprises *an encryption of a first random value and a hash of the first random value*". Accordingly, the Applicant respectfully requests that the Patent Office allow Claim 92 and its dependent claims.

Claims 93—96 depend from Claim 92 and are allowable as depending from an allowable base claim. These claims are also allowable for their own

recited features that, in combination with those recited in Claim 92, are neither disclosed nor suggested in references of record, either singly or in combination with one another.

Claims 97—124 are allowable for at least the reasons that claims 83—96 are allowable.

Conclusion

The arguments presented above are intended to present the Applicant's position clearly, but should not be considered exhaustive. Accordingly, the Applicant reserves the right to present additional arguments to clarify the Applicant's position further. Moreover, the Applicant reserves the right to challenge the status as prior art of one or more documents cited in the Office Action.

The Applicant submits that the claims as presented are in condition for allowance. Accordingly, the Applicant respectfully requests that a Notice of Allowability be issued. If the Patent Office's next anticipated action is not the issuance of a Notice of Allowability, the Applicant respectfully requests that the undersigned attorney be contacted to schedule an interview.

Respectfully Submitted,

Dated: 2-13-06 By: _____

David S. Thompson
Reg. No. 37,954
Attorney for Applicant

LEE & HAYES PLLC
Suite 500
421 W. Riverside Avenue
Spokane, Washington 99201
Telephone: 509-324-9256 x235
Facsimile: (509) 323-8979